**CIS 2640 - Lab 13**

**Secure Network Administration Principles Log Analysis**

| **Your Name:** | Liliane Owens |
| --- | --- |
| **Date:** | 4/7/2023 |

**Instructions**: Complete the exercises included on this worksheet. For each exercise, read the instructions, complete the required tasks and submit evidence of your completed tasks (a screen shot is your evidence), and then answer the question provided.

* **Showing Evidence of Completion:** Your evidence of completion is a screen shot, as described in each exercise. Use the tool of your choice to take a screen shot of the required content. Paste the screen shot into the table cell as indicated. Make your screen shot image small by clicking on it, then holding down the SHIFT key while dragging one of the corner nodes inward. Your instructor will resize the images as needed to review your work.
* **Answering Questions:** Your answers should be written in carefully edited college-level English, using complete sentences.

| **Lab – Secure Network Administration Principles Log Analysis** | |
| --- | --- |
| **Instructions and Evidence of Completion** | **Answer a Question** |
| At the end of this document (not within this table) paste screen captures that show:   1. A successful Parsing FTP with Scripts by just showing the port numbers. 2. Using the grep command to show entries with Firefox 3. The Output of Hydra cracking the FTP password.   ***Be sure your screen shot(s) include any command executed and the resulting output in clear / cropped screenshots.*** | Question(s): Answer each of the questions below; use the space to the right of each question for your answer. Make sure your answers are clear and complete. |
| ***Questions*** | ***Answers*** |
| 1. What command line syntax would did you enter to show output for a specific IP address? | **/home/scripts/scanreport.sh -f parsed.txt -i 192.168.1.50** |
| 1. Why would you need to parse Nmap reports? | It makes it easy to read the format. |
| 1. How do you grep for the word *nmap* within the *access\_log*? | Using this command cat access.log | grep Nmap |
| 1. What command was used to generate noise on the network. | **nmap -T4 -A -v 192.168.1.50.** |
| 1. What command was used to add groups in Kali Linux? | **groupadd anongroup** |
| 1. What is Hydra? | Hydra is a brute-force tool that helps us to crack passwords of network services. It can perform rapid dictionary attacks against more than 50 protocols. |
| 1. Hydra used a dictionary attack against the remote system, where is the password list located that was used? | It was located in **/tmp/wordlists/passlist**. |

Put screenshots here:

1. A Successful Parsing FTP with Scripts by just showing the port numbers.

![A picture containing timeline

Description automatically generated]()

1. Using the grep command to show entries with Firefox.

![Text

Description automatically generated]()

1. The Output of Hydra cracking the FTP password.

![Graphical user interface, text, application, email

Description automatically generated]()